DATA PROCESSING AGREEMENT

Last updated version: January 26th, 2026

This Data Processing Agreement ("DPA") shall apply to all Subscription Agreements in which QUALIFYZE GMBH or QUALIFYZE INC. (hereinafter individually each as "Qualifyze"), in the course of fulfilling its obligations under the relevant Subscription Agreement, processes Personal Data on behalf of a client acting as a Data Controller. Qualifyze is also referred to as "Data Processor" and the respective client as "Data Controller"; they are also referred to collectively as the "Parties" and each as a "Party". For the avoidance of doubt, if the Client has a Subscription Agreement in place with Qualifyze, the Data Processor is the company the Client has signed the Subscription Agreement with.

1. Definitions and Interpretation

(1) Unless otherwise defined herein, capitalized terms and expressions used in this DPA shall have the same meaning as in the General Data Protection Regulation 2016/679 ("GDPR") or the Subscription Agreement and their cognate terms shall be construed accordingly.

(2) In addition, the following definitions shall be applicable:

a) "**Affiliated Company**" or "**Affiliated Companies**" shall mean any company directly or indirectly owning or controlling any Party, or any company under the same direct or indirect ownership or control as any Party, or any company directly or indirectly owned or controlled by any Party. Ownership or control shall exist through the direct or indirect ownership or control of more than 50% of the nominal value of the issued equity share capital or of more than 50% of the shares entitling the holders to vote for the appointment of directors or persons performing similar functions. Ownership or control shall also exist when there is power to direct or cause the direction of the management or policies of the company by any means.

b) **"Auditor"** shall mean the independent, qualified and experienced auditors in accordance with international quality standards, hired by Qualifyze.

c) **"Auditee"** shall mean the Client's supplier.

d) "**Data Protection Laws and Regulations**" means all applicable and binding privacy and data protection laws.

e) "**FADP**" means the Federal Act on Data Protection of 19 June 1992, and as revised as of 25 September 2020, which entered into force on 1 September 2023 (the "Revised FADP")

f) "**UK GDPR**" means the Data Protection Act 2018, as well as the GDPR as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018 and as amended by the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019 (SI 2019/419).

g) **"UK Representative"** means the representative appointed by the relevant Party, as applicable, in the United Kingdom in accordance with Article 27 of the UK GDPR.

h) **"KVKK"** means the Law on Protection of Personal Data No.6698 of the Republic of Turkey, together with its secondary regulations, guidelines, and any subsequent amendments issued by the Turkish Data Protection Authority.

i) "**Standard Contractual Clauses**" means (a) in respect of transfers of Personal Data subject to the GDPR, the standard contractual clauses between controllers and processors, and between processors and processors (as applicable), as approved by the European Commission Implementing Decision (EU) 2021/914 of 4 June 2021, including all annexes

thereto ("EU SCCs") as set out in Part 1 of APPENDIX IV of this DPA; (b) in respect of transfers subject to the Federal Act on Data Protection (Revised FADP), the terms set forth in Part 2 of APPENDIX IV hereto ("Switzerland Addendum").(c) in respect of transfers of Personal Data subject to the UK GDPR, the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses of 21 March 2022 (version B.1.0), as incorporated into the EU SCCs through Part 3 of APPENDIX IV ("UK Addendum"); (d) in respect of transfers subject to the KVKK, the term sets forth in part 4 of APPENDIX IV and

j) "**Sensitive Personal Data**" means Personal Data that is protected under a special legislation and requires unique treatment, such as "special categories of data", "sensitive data" or other materially similar terms under applicable Data Protection Laws.

k) "**Sub-Processor**" means any third party that Processes Personal Data under the instructions or supervisions of Qualifyze.

2. Personal Data

(1) The Data Processor shall process Personal Data on behalf of the Data Controller in accordance with the written instructions given by the Data Controller.

(2) A description of the categories of Personal Data and Data Subjects and the processing activities can be found in Appendix I.

(3) The Parties acknowledge and agree that, except for health data as stated in Appendix I (if applicable), no other categories of Sensitive Data are intended to be Processed under this DPA. The processing of health data is limited to what is strictly necessary for the performance of the Services. The Data Controller represents and warrants that it has obtained all necessary consents, or other lawful bases, as required under applicable Data Protection Law and Regulation, for the lawful Processing of such health data by the Processor.

3. Processing of Personal Data

(1) The Data Processor shall comply with all Data Protection laws applicable to it in the Processing of Personal Data and process the Personal Data only in line with the instructions issued by the Data Controller, including with regard to transfers of Personal Data to a third country or an international organisation, unless required to do so by Union or Member State law to which the Data Processor is subject; in such a case, the processor shall inform the Data Controller or that the legal requirement before processing, unless that law prohibits such information on important grounds of public interest;

4. Data Processor's Personnel

(1) The Data Processor shall take reasonable steps to ensure the reliability of any employee, agent or contractor who may have access to the Data Controller's Personal Data, ensuring that access is strictly limited on a need-to-know basis, and strictly necessary for the purposes of the applicable Subscription Agreement.

(2) Likewise, Data Processor shall ensure that the persons authorised to process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory or contractual obligation of confidentiality.

5. Security

(1) Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the Data Processor shall implement the appropriate

technical and organizational measures to ensure an appropriate level of security as established in article 32 of the GDPR, and equivalent requirements under the Applicable Laws and Regulations, including as appropriate:

a. The pseudonymization and encryption of Personal Data.
b. The ability to ensure the ongoing, confidentiality, integrity, availability and resilience of processing systems and services;
c. The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
d. A process for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

(2) In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data transmitted, stored or otherwise processed.

(3) The technical and organizational measures employed by the Data Processor are described in Appendix II.

6. Relationship between Qualifyze GmbH and Qualifyze Inc.

(1) For the avoidance of doubt, under a Subscription Agreement, both Qualifyze entities may act either as (i) Data Processor, when directly engaged under a Subscription Agreement; or (ii) sub-processor, when providing limited support and maintenance services to the other Qualifyze entity for fulfilment of such Subscription Agreement.

(2) In such cases, the Qualifyze entity with whom the Client signed the Subscription Agreement shall remain the main Data Processor towards the Client, and the other Qualifyze entity shall be bound by equivalent data protection obligations as those set forth in this DPA.

(3) For the avoidance of doubt, data processing activities jointly carried out by Qualifyze GmbH and Qualifyze Inc. as joint controllers (e.g., users of the Qualifyze platform) are governed by a separate Joint Controllership Agreement between both companies.

7. Sub processing

(1) The Data Processor may engage other processors (“subprocessors”) to provide auxiliary or essential services necessary for the normal operation of the services, including but not limited to hosting, storing, analytics, communication tools, and infrastructure services.

The Data Controller hereby grants the Data Processor a general written authorisation, in accordance with article 28(2) GDPR, to engage such other processors (including any Affiliate of the Data Processor or Qualified Auditor).A current list of authorized subprocessors is maintained and publicly available as Appendix III.

(2) Notwithstanding the foregoing, the Data Processor shall inform the Data Controller of any intended additions or replacement of processors by updating the publicly available list. The Data Controller may raise a reasonable and justified objection to a new sub-processor within 14 calendar days from the date of publication. The objection must be based on substantiated concerns regarding the subprocessor’s ability to ensure adequate data protection.

(3) The Data Processor shall ensure that all subprocessors are bound by contractual terms that impose obligations equivalent to those set out in this DPA, including sufficient guarantees regarding the implementation of appropriate technical and organizational measures. The Data Processor remains fully liable to the Data Controller of any breach of the data protection laws by its subprocessors in accordance with clause 7 of the Subscription Agreement.

(4) In cases where a subprocessor is located in a third country not recognised as providing an adequate level of protection under GDPR, the Data Processor shall ensure that such data transfers are subject to appropriate safeguards in accordance with Article 46 GDPR, including the use of the Standard Contractual Clauses (Commission Decision (EU) 2021/914, Module 3 – Processor to Processor), or equivalent legal instruments..

8. Data processor's Obligations

(1) Taking into account the nature of the processing, the Data Processor undertakes to assist the Data Controller by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of the Data Controller's obligation to respond a Data Subject Request under Data Protection Laws and Regulations. In particular, the Data Processor shall:

a. Promptly notify the Data Controller if it receives a request from a Data Subject under any data protection law in respect of the Data Controller's Personal Data; and

b. Undertakes not to respond to that request except on the documented instructions of the Data Controller or as required by applicable law to which the Data Processor is subject, in which case the Data Processor shall inform the Data Controller of that legal requirement before responding to the request.

(2) To the extent required under applicable Data Protection Laws and Regulations,the Data Processor shall notify the Data Controller without undue delay and, where feasible, within 48 hours of becoming aware of a Personal Data Breach affecting the Data Controller's Personal Data, providing the Data Controller with sufficient information to allow the Data Controller to meet any obligations to report or inform Data Subjects of the Personal Data Breach. Data Processor shall co-operate with the Data Controller and take reasonable commercial steps as directed by the Data Controller to assist in the investigation, mitigation and remediation of each such Personal Data Breach.
Said notification shall at least:

a. Describe the nature of the personal data breach including where possible, the categories and approximate number of Data Subjects concerned and the categories and approximate number of Personal Data records concerned;

b. Communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;

c. Describe the likely consequences of the Personal Data Breach;

d. Describe the measures taken or proposed to be taken by the Data Controller to address the Personal Data Breach, including, where appropriate, measures to mitigate its possible adverse effects.

Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay. In any event the Data Controller will be the Party responsible for notifying relevant Supervisory Authority(ies) and/or concerned data subjects where required by Data Protection Laws and
In no case will the Data Processor notify the Personal Data Breach to the supervisory authority competent without the authorization of the Data Controller.

(3) The Data Processor shall co-operate with the Data Controller with any Data Protection Impact Assessment which the data Controller reasonably considers to be subject to pursuant to Article 35 GDPR.

9. Term and Termination

(1) This DPA shall become effective on the same date as the Subscription Agreement and shall remain in force until the Subscription Agreement is terminated in accordance with its terms.

(2) Upon written request from the Data Controller, the Data Processor will, within 30 business days, return to the Data Controller all documents and other materials in the Data Processor's possession containing Personal Data of the Data Controller. The Data Controller might, at its sole discretion, request the Data Processor to destroy all documents and other materials in the Data Processor's possession containing Personal Data of the Data Controller.

(3) Notwithstanding the foregoing, (a) the Data Processor may retain one copy of all documents and other materials containing Personal Data of the Data Controller for archival, compliance and legal purposes, and (b) the Data Processor shall not be required to destroy any securely stored

computer files that contain Personal Data of the Data Controller created during automatic system back-ups and/or archiving systems.

10. International Data Transfer

For Clients with an active Subscription Agreement with Qualifyze GmbH: Personal Data may be transferred from EU Member States, the EEA member countries ("EEA"), Switzerland, the United Kingdom ("UK"), or to countries that offer an adequate level of data protection pursuant to the adequacy decisions published by the relevant Data Protection Authorities ("Adequacy Decisions"), as applicable, without any further safeguard being necessary. If, for the provision of the services, Processing of Personal Data includes transfers from the EEA, Switzerland, the UK, or the Republic of Turkey to other countries which have not been subject to a relevant Adequacy Decision; then (i) the terms set forth in Part 1 of Appendix IV (EEA Cross Border Transfers) shall apply to any such EEA Transfer, (ii) the terms set forth in Part 2 of Appendix IV (Switzerland Cross Border Transfers) shall apply to any such Swiss Transfer, (iii) the terms set forth in Part 3 of Appendix iv (UK Cross-Border Transfers) shall apply to any such UK transfer, and (iv) the terms set forth if Part 4 of Appendix IV (Turkey Cross-Border Transfers) shall apply to any such Cross-Border Transfers.(v) the terms set forth if Part 5 of Appendix IV (Additional Safeguards) shall apply to any such Cross-Border Transfers.

For Clients with an active Subscription Agreement with Qualifyze Inc.: The Parties acknowledge that, although both entities are established in the United States, the processing of personal data under this DPA may involve the transfer of personal data originating from the European Economic Area (EEA). The Parties agree that such transfer will be governed by the Standard Contractual Clauses adopted by the European Commission's Implementing Decision (EU) 2021/914, Module IV included as an exhibit herein.

11. Personal Data of the Signatories and other Contact Persons

(1) The signatories and the contact persons are informed that their personal data will be processed by both Parties as independent controllers. Both Parties shall observe any applicable data protection regulation, in particular the provisions of the GDPR. The legal basis for the processing is the performance of the contract.The data may be transferred to the Affiliates of Qualifyze for administrative purposes only.

(2) The data subject may exercise the rights to access, rectification or erasure of the data, restriction of processing and portability, as well as withdraw the consent, without affecting the lawfulness of the processing based on consent before its withdrawal, by sending a written request to the Data Controller, whose contact details are in the corresponding Subscription Agreement. They may also lodge a complaint with the competent supervisory authority in accordance with the applicable Data Protection Laws and Regulations. The data will be stored for the duration of the contractual relationship and even after the termination until the appropriate legal actions for this purpose expire.

12. Miscellaneous

(1) Each Party must keep this DPA and information it receives about the other Party and its business in connection with this DPA ("Confidential Information") confidential and must not use or disclose that Confidential Information without the prior written consent of the other Party except to the extent that: (a) disclosure is required by law; (b) the relevant information is already in the public domain (c) can be proven by the receiving Party to have been developed independently of Confidential Information received from the disclosing Party; or (d) are approved in writing by the disclosing Party not to be treated as confidential.

(2) No Party may assign any rights or claims under this DPA without the prior written consent of the other Party (within the meaning of section 126 b German Civil Code). This will not apply to assignments to Affiliated Companies of the assigning Party or successors of the Parties.

(3) This DPA comprises the entire agreement between the Parties concerning its subject matter. It shall supersede all prior agreements and conventions, oral and written declarations of intent and other arrangements or side agreements (whether binding or non-binding) made by the Parties in respect thereof. This does not apply to a confidentiality agreement concluded between the Parties. In case of a conflict between any Contractual Document, including the Subscription Agreement, and the provisions of this DPA, the provisions of this DPA shall prevail.

(4) No amendments to this DPA shall be valid and binding unless they are in writing and signed by the Parties.

(5) The failure or delay by the either Party in exercising or enforcing any right, remedy or power under this Subscription Agreement shall not constitute or operate as a waiver of that right, remedy or power. The single or partial exercise or enforcement of any right, remedy or power under this DPA shall not preclude or restrict any further exercise or enforcement of that right, remedy or power, or the exercise or enforcement of any other right, remedy or power under this DPA.

(6) Should one or more provisions of the DPA be or become invalid or unenforceable, this shall not affect the validity and enforceability of the remaining provisions of the DPA. In that case, the Parties shall agree a valid provision to replace the invalid or unenforceable provision which reflects as closely as possible the original economic purpose, provided a supplementary interpretation of the DPA does not have precedence or is not possible. In place of the invalid or unenforceable provision, or to fill a contractual lacuna, such valid and enforceable provision shall apply which reflects as closely as possible the commercial intention of the Parties as regards the invalid, unenforceable or missing provision.

(7) Each Party represents and warrants to the other Party that it has the legal power and authority to enter into and perform under this DPA.

(8) The Parties agree that electronic signatures, if used in execution of this DPA, any subsequent amendments and/or any Contractual Document, are legally binding and have the same legal effect as traditional handwritten/wet ink signatures. Each of the Parties agrees that the electronic signatures used in execution of this DPA, any subsequent amendments and/or any Audit Contracts shall constitute an original for all purposes. The Parties also agree that exchanging scanned copies of this DPA, any subsequent amendments and/or any Contractual Documents containing traditional handwritten/wet ink signatures via email is legally binding and has the same legal effect as exchanging hard copies of the DPA.

APPENDIX I DESCRIPTION OF DATA SUBJECTS AND DATA PROCESSING ACTIVITIES

Affected persons and group of persons	In particular: ● Contact persons and employees of Data Controller ● Contact persons and employees of Data Controller's suppliers Where Data Importer's supplier conduct clinical trials that are within the scope of the audit at hand: ● Participants of clinical trials
Type of data or data categories	In particular: ● Full name ● E-mail address ● Phone number ● Job Title Where Data Importer's supplier conduct clinical trials that are within the scope of the audit at hand: ● Health data (pursuant to Art. 9 GDPR)
Nature and purpose of processing	Nature of the processing: ● Collection, use, storage and deletion of personal data Purpose of the processing: ● Provision of Data Processor's services via the Internet (*i.e.*, SaaS distribution), in particular ● Facilitation and conduction of audits of Data Processor's client suppliers via selected auditors

APPENDIX II TECHNICAL AND ORGANIZATIONAL MEASURES (TOMS)IN ACCORDANCE WITH ART. 32 GDPR

SECTION 1. PURPOSE AND APPLICABILITY

A secure personal data processing is fundamental to Qualifyze's operational efficiency, risk mitigation, and overall health. This document describes the technical and organizational measures Qualifyze takes with regards to the processing of personal data in accordance with article 32 of the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, on the protection of natural persons with regards to the processing of personal data and on the free movement of such data (hereinafter "GDPR").

SECTION 2. ANONYMIZATION, PSEUDONYMIZATION AND ENCRYPTION:

Encryption: all devices with access to personal data shall be encrypted. Client information when at rest and in transit, or stored on portable devices shall be encrypted to avoid access for unauthorized individuals.

- Data rest is encrypted using AWS Key Management Service (KMS) with symmetric keys (key spec: symmetric_default), utilizing the AES-256 encryption algorithm as per AWS standards.
- Data in transit is encrypted using RSA 2048-bit encryption provided by Amazon for secure communication over its web applications.

SECTION 3. CONFIDENTIALITY:

3.1. **Access Control:** Qualifyze has established robust and secured access through one-person passwords and permissions control.

3.1.1. **Passwords**: for every network user, a personally assigned user must be set up with a minimum of 8-digit password featuring both uppercase and lowercase letters, numbers, and special characters, in accordance with the OWASP recommendations.

3.1.2. **Access restrictions**: Qualifyze's access to networks and applications are built on the principle of the minimum privilege. Authorizations are implemented through a role-based access control (RBAC), ensuring that Qualfiyze's employees and users have access only to the data and resources necessary for their roles. Creating, changing, and removing authorizations is managed in documented procedures and monitoring of administrator access is performed continuously using advanced security tools. Systems are protected by VPN and all cloud accounts shall require a two-factor authentication mechanism. Auth0 for identity management with a 2FA for internal users is applied.

3.1.3. **Logging and Monitoring**: Access logs are maintained and regularly reviewed to detect any unusual or unauthorised activities. Automated alerts are configured to notify security personnel of any suspicious access attempts or anomalies.

3.2. **Entry Control:** The physical offices in which personal data are processed shall not be freely accessible, rooms must be locked when employees are away. In cases of remote access to personal data, Qualifyze's security policies shall apply and shall be done using a multi-factor authentication method.

3.2. **Transition control:** controls to prevent the transition of data to external systems shall be in place. Environments shall be isolated in separate networks.

3.3. **Confidential Disclosure Agreements:** all employees and third parties allowed to access personal data are bound by confidentiality obligations under formal agreements.

3.4. **Security:** Network firewalls, website filtering, intrusion prevention/detection solutions are in place.

SECTION 4. INTEGRITY AND AVAILABILITY:

4.1. **Devices and Software management:** personal data shall be processed on data processing systems that are subject to regular and documented patch management. A state of the art firewall is enabled by default and is kept up to date. Servers shall be replicated in the cloud in order to ensure availability. Automatic scripts that apply backups shall be used, as well as infra as code.

4.2. **Logging and monitoring:** access logs are maintained to ensure traceability of access, modifications to personal data and deletions are recorded. Regular integrity checks and hashing mechanisms are in place to detect unauthorized alterations.

4.3. **Backups:** backups of essential personal data are performed on a regular basis according to Qualifyze's internal policies and industry best practices. Qualifyze regularly tests the backup process, at least once per quarter.

4.4. **Testing:** regular vulnerability scannings and penetration testings are conducted.

4.5. **Disaster recovery** and **business continuity plans** are in place.

SECTION 5. INCIDENT RESPONSE:

Qualifyze has a documented security incident management protocol that covers incident response, escalation and remediation to ensure availability to restore the availability and access to personal data in a timely manner. Records of incidents are retained for a minimum of 5 years. Security incidents involving Client's personal data will be notified in accordance with clause 7 of the DPA.

SECTION 6. DATA DELETION:

Client personal data shall be deleted from Qualifyze information systems upon written request by the Client when no longer needed by Qualifyze to fulfill its obligations under the subscription agreement.

SECTION 7. REVIEW AND EVALUATION:

Qualifyze TOMs are periodically reviewed to assess compliance with industry security standards and applicable regulations, regular audits are conducted. Upon Client's request, when deemed appropriate by Qualifyze, Qualifyze will provide relevant information to the client to demonstrate compliance with this TOMs.

APPENDIX III – LIST OF SUB-PROCESSORS

- *Amazon Web Services (hosting and infrastructure), Germany.*
- *Google (Data hosting provider), Germany.*
- *Microsoft (Office 365 and OneDrive Suite), Germany.*
- *JIRA and Confluence from Atlassian (project management), Ireland.*
- *Make (Data automation flows), Germany.*
- *HubSpot (Customer Relationship Management – CRM), Germany.*
- *Mailchimp (Email Marketing), USA.*
- *Hotjar (analyze user behaviour on websites), Ireland.*
- *DataDog Inc. (security and system maintenance), Europe.*
- *AirTable, (support tool), US.*
- *Slack (internal messaging system), Germany.*
- *Qualifyze Spain, S.L.U. (Service & Support), Spain.*
- *Qualifyze Inc. (Service & Support), US. - acts as a sub-processor only when the Subscription Agreement has been signed with Qualifyze GmbH.*
- *Qualifyze GmbH (Service & Support), Germany - acts as a sub-processor only when the Subscription Agreement has been signed with Qualifyze Inc.*
- *Qualified auditors as agreed with the Client in accordance with the Subscription Agreement.*
- *Gong.io, (notetaker of meetings with clients for training and quality purposes), Israel, US, UK, EEA.*
- *ChiliPiper (scheduling services), US.*
- *DocuSign Inc., (signing tool) EEA, (depending on the DocuSign account used).*
- *Juro Online Limited, (contract automation), Ireland.*
- *Fivetran Inc., (automated data integration), US.*

APPENDIX IV

PART 1.- EEA CROSS BORDER TRANSFERS

STANDARD CONTRACTUAL CLAUSES

Module IV (Processor to Controller)

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) ([1]) for the transfer of personal data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer')

have agreed to these standard contractual clauses (hereinafter: 'Clauses').

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or

---

[1] Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision 2021/915.

additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8.1 (b) and Clause 8.3(b);

(iii) N/A

(iv) N/A

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18.

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7 – Optional

Docking clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Instructions

(a) The data exporter shall process the personal data only on documented instructions from the data importer acting as its controller.

(b) The data exporter shall immediately inform the data importer if it is unable to follow those instructions, including if such instructions infringe Regulation (EU) 2016/679 or other Union or Member State data protection law.

(c) The data importer shall refrain from any action that would prevent the data exporter from fulfilling its obligations under Regulation (EU) 2016/679, including in the context of sub-processing or as regards cooperation with competent supervisory authorities.

(d) After the end of the provision of the processing services, the data exporter shall, at the choice of the data importer, delete all personal data processed on behalf of the data importer and certify to the data importer that it has done so, or return to the data importer all personal data processed on its behalf and delete existing copies.

8.2 Security of processing

(a) The Parties shall implement appropriate technical and organisational measures to ensure the security of the data, including during transmission, and protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access (hereinafter 'personal data breach'). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature of the personal data ([2]), the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects, and in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner.

(b) The data exporter shall assist the data importer in ensuring appropriate security of the data in accordance with paragraph (a). In case of a personal data breach concerning the personal data processed by the data exporter under these Clauses, the data exporter shall notify the data

[2] This includes whether the transfer and further processing involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions or offences.

importer without undue delay after becoming aware of it and assist the data importer in addressing the breach.

(c) The data exporter shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

8.3 Documentation and compliance

(a) The Parties shall be able to demonstrate compliance with these Clauses.

(b) The data exporter shall make available to the data importer all information necessary to demonstrate compliance with its obligations under these Clauses and allow for and contribute to audits.

Clause 9

Use of sub-processors

N/A

Clause 10

Data subject rights

The Parties shall assist each other in responding to enquiries and requests made by data subjects under the local law applicable to the data importer or, for data processing by the data exporter in the EU, under Regulation (EU) 2016/679.

Clause 11

Redress

The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

Clause 12

Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) Each Party shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages that the Party causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter under Regulation (EU) 2016/679.

(c) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(d) The Parties agree that if one Party is held liable under paragraph (c), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(e) The data importer may not invoke the conduct of a processor or sub-processor to avoid its own liability.

Clause 13

Supervision

N/A

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

(where the EU where the EU processor combines the personal data received from the third country-controller with personal data collected by the processor in the EU)

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards ([3]);

[3] As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

(where the EU processor combines the personal data received from the third country-controller with personal data collected by the processor in the EU)

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much

information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data collected by the data exporter in the EU that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall immediately be deleted in its entirety, including any copy thereof. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

These Clauses shall be governed by the law of a country allowing for third-party beneficiary rights. The Parties agree that this shall be the law of Germany.

Clause 18

Choice of forum and jurisdiction

Any dispute arising from these Clauses shall be resolved by the courts of Frankfurt am Main, Germany.

Qualifyze

ANNEX I

A. LIST OF PARTIES

Data exporter(s): [*Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]*

Name: Qualifyze GmbH (if the Subscription Agreement has been signed with this entity) or Qualifyze Inc. (if the Subscription Agreement has been signed with this entity).

Address: Bockenheimer Anlage 46, 60322, Frankfurt am Main, Germany and 525 Washington Blvd, Jersey City, NJ 7310, New Jersey, United States (respectively)

Contact person's name, position and contact details: Rosa de Antonio Rodríguez, Data Protection Officer; dataprivacy@qualifyze.com (Qualifyze GmbH) and dataprivacy@qualifyze.com (Qualifyze Inc.)

UK Representative (if applicable)

Ametros Group Ltd, Broadway House, 32-35 Broadstreet, Hereford, England, HR4 9AR; gdpr@ametrosgroup.com , for detailed information : www.ametrosgroup.com

Activities relevant to the data transferred under these Clauses:

Transfer of audit reports pursuant to contract obligations to Data Importer as further described in the DPA.

Signature and date:

Role (controller/processor): Processor

Data importer(s): [*Identity and contact details of the data importer(s), including any contact person with responsibility for data protection]*

Name: As laid down in the Subscription Agreement

Address: As laid down in the Subscription Agreement and/or order form

Contact person's name, position and contact details: As laid down in the Subscription Agreement and/or order form

Activities relevant to the data transferred under these Clauses:

Use and disclosure of audit reports to relevant authorities; storage of audit reports pursuant to statutory retention obligations.

Signature and date:

Role (controller/processor): Controller

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

- Contact persons and employees of Data Importer's supplier
- Where audited entities conducted clinical trials: participants of said clinical trials

Categories of personal data transferred

Contact data, e.g. full name, e-mail address, phone number.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

Where audited entities conducted clinical trials: health data relating to participants of said clinical trials. The sensitive data is only transferred and used further by the Data Importer as part of the audit reports and only disclosed to relevant authorities pursuant to statutory obligations.

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

Continuous basis

Nature of the processing

Storage, combination, dissemination

Purpose(s) of the data transfer and further processing

Transfer to Data Controller as part of audit results pursuant to contract obligations as further described in the DPA.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

Only for as long as required by applicable statutory retention obligations.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

n/a

PART 2 - SWITZERLAND CROSS BORDER TRANSFERS

The Parties agree that the Standard Contractual Clauses approved by the European Commission (EU) 2021/914, of June 4th, 2021, incorporated herein as Part 1 of Appendix IV, shall be adjusted as set out below where the Federal Act on Data Protection of 19 June 1992 (the "FADP", and revised as of 25 September 2020, the "Revised FADP") applies to Switzerland Transfers: In the event of any conflict between the DPA and this Addendum, this Addendum shall prevail only to the extent necessary to comply with the FADP.

References to the EU SSCs means the EU SCCs as amended by this Part 2;

(1) The Swiss Federal Data Protection and Information Commissioner ("FDPIC") shall be the sole Supervisory authority for Switzerland Transfers exclusively subject to FADP;

(2) The terms "General Data Protection Regulation" or "Regulation (EU) 2016/679" as utilized in the Standard Contractual Clauses shall be interpreted to include the FADP with respect to Switzerland Transfers.

(3) Switzerland Transfers subject to both the FADP and the GDPR, shall be dealt with by the EU Supervisory Authority named in Part 1 of this APPENDIX IV.

(4) References to the "Union", "EU" and "EU Member State" shall not be interpreted in such a way as to exclude Data Subjects in Switzerland from the possibility of exercising their rights in their place of habitual residence (Switzerland) in accordance with Clause 18(c) of the EU SCCs;

(5) All references to Member State(s)/EU Member State(s) shall be deemed to include Switzerland.

(6) All references to the importer in the EU shall be deemed to include the importer in Switzerland.

(7) Where Switzerland Transfers are subject to both the FDPA and the EU GDPR, all references to the GDPR in the Standard Contractual Clauses are to be understood to include references to the FDPA insofar as the Switzerland Transfers are subject to the FADP.

PART 3 – UK Cross Border Transfers

This PART 3 applies where personal data is transferred in accordance with the UK GDPR.

Table 1: The Parties: as detailed in Annex I of Part 1 of this APPENDIX IV.

Table 2: Selected SCCs, Modules and Selected Clauses: as detailed in Part 1 of this APPENDIX IV.

Table 3: Appendix Information: means the information which must be provided for the selected modules as set out in the Appendix of the Standard Contractual Clauses (other than the Parties), and which is set out in Part 1 of this APPENDIX IV.

Entering into this Part 3:

1. Each Party agrees to be bound by the terms and conditions set out in this Part 3, in exchange for the other Party also agreeing to be bound by this Part 3.

2. Although Annex 1A and Clause 7 of the Standard Contractual Clauses require signature by the Parties, for the purpose of making UK Transfers, the Parties may enter into this Part 3 in any way that makes them legally binding on the Parties and allows data subjects to enforce their rights as set out in this Part.

3. Entering into this Part 3 will have the same effect as signing the Standard Contractual Clauses and any part of the Standard Contractual Clauses.

Interpretation of this Part 3:

(1) Where this Part 3 uses terms that are defined in the Standard Contractual Clauses, those terms shall have the same meaning as in the Standard Contractual Clauses. In addition, the following terms have the following meanings:

Addendum EU SCCs	**The version(s) of the Standard Contractual Clauses to which this Part 3 is appended, as set out in Table 2, including the Appendix Information.**
Appropriate Safeguards	**The standard of protection over the personal data and of data subjects' rights, which is required by UK Data Protection Laws when the Parties are making a UK Transfer relying on standard data protection clauses under Article 46(2)(d) UK GDPR.**
ICO	**The Information Commissioner.**

Part 3	**This Part 3 which is made up of this Part 3 incorporating the Addendum EU SCCs.**
UK Addendum	**An addendum to the Standard Contractual Clauses published by the ICO and approved by the UK Parliament.**
UK Data Protection Laws	**All laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018.**
UK GDPR	**As defined in Section 3 of the Data Protection Act 2018.**
UK	**The United Kingdom of Great Britain and Northern Ireland.**
UK Transfer	**A transfer which is covered by Chapter V of the UK GDPR.**

(2) This Part 3 must always be interpreted in a manner that is consistent with UK Data Protection Laws and so that it fulfils the Parties' obligation to provide the Appropriate Safeguards.
(3) If the provisions included in the Addendum EU SCCs amend the Standard Contractual Clauses in any way which is not permitted under the Standard Contractual Clauses or this Part 3, such amendment(s) will not be incorporated by this Part 3 and the equivalent provision of the Standard Contractual Clauses will take their place.
(4) If there is any inconsistency or conflict between UK Data Protection Laws and this Part 3, UK Data Protection Laws applies.
(5) If the meaning of this Part 3 is unclear or there is more than one meaning, the meaning which most closely aligns with UK Data Protection Laws applies.
(6) Any references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, reenacted and/or replaced after this DPA has been entered into.

Hierarchy:

(1) Although Clause 5 of the Standard Contractual Clauses sets out that the Standard Contractual Clauses prevail over all related agreements between the Parties, the Parties agree that, for a UK Transfer, the hierarchy in Section 10 will prevail.

(2) Where there is any inconsistency or conflict between this Part 3 and the Addendum EU SCCs (as applicable), this Part 3 overrides the Addendum EU SCCs, except where (and in so far as) the inconsistent or conflicting terms of the Addendum EU SCCs provides greater protection for data subjects, in which case those terms will override the provisions of this Part 3.
(3) Where this Part 3 incorporates Addendum EU SCCs which have been entered into to protect transfers subject to the General Data Protection Regulation (EU) 2016/679 then the Parties acknowledge that nothing in this Part 3 impacts those Addendum EU SCCs.

Incorporation and changes to the Standard Contractual Clauses:

(1) This Part 3 incorporates the Addendum EU SCCs which are amended to the extent necessary so that:
    (a) together they operate for data transfers made by the data exporter to the data importer, to the extent that UK Data Protection Laws apply to the data exporter's processing when making that data transfer, and they provide Appropriate Safeguards for those data transfers;
    (b) Sections 9 to 11 override Clause 5 (Hierarchy) of the Standard Contractual Clauses; and
    (c) this Part 3 (including the Addendum EU SCCs incorporated into it) is (1) governed by the laws of England and Wales and (2) any dispute arising from it is resolved by the courts of England and Wales, in each case unless the laws and/or courts of Scotland or Northern Ireland have been expressly selected by the Parties.
(2) Unless the Parties have agreed alternative amendments which meet the requirements of Section 12, the provisions of Section 15 below will apply.
(3) No amendments to the Standard Contractual Clauses other than to meet the requirements of Section 12 may be made.
(4) The following amendments to the Addendum EU SCCs (for the purpose of Section 12) are made:
    (a) References to the "Clauses" means this Part 3, incorporating the Addendum EU SCCs;
    (b) In Clause 2, delete the words:

        "and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679";

    (c) Clause 6 (Description of the transfer(s)) is replaced with:

        "The details of the transfers(s) and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred) are those specified in Annex I.B where UK Data Protection Laws apply to the data exporter's processing when making that transfer.";

    (d) References to "Regulation (EU) 2016/679", "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)" and "that

Regulation" are all replaced by "UK Data Protection Laws". References to specific Article(s) of "Regulation (EU) 2016/679" are replaced with the equivalent Article or Section of UK Data Protection Laws;

(e) References to the "European Union", "Union", "EU", "EU Member State", "Member State" and "EU or Member State" are all replaced with the "UK";

(f) Clause 13(a) and Part C of Annex I are not used;

(g) The "competent supervisory authority" and "supervisory authority" are both replaced with the "Information Commissioner";

(h) In Clause 16(e), subsection (i) is replaced with:

"the Secretary of State makes regulations pursuant to Section 17A of the Data Protection Act 2018 that cover the transfer of personal data to which these clauses apply;";

(i) Clause 17 is replaced with:

"These Clauses are governed by the laws of England and Wales.";

(j) Clause 18 is replaced with:

"Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts.";

(k) The footnotes to the Standard Contractual Clauses do not form part of this Part 3, except for footnotes 8, 9, 10 and 11.

<u>Amendments to this Part 3</u>

(1) The Parties may agree to change Clause 17 and/or 18 of this Part 3 to refer to the laws and/or courts of Scotland or Northern Ireland.

(2) If the Parties wish to change the format of the information included in Tables 1, 2 or 3 of this Part 2, they may do so by agreeing to the change in writing, provided that the change does not reduce the Appropriate Safeguards.

(3) From time to time, the ICO may issue a revised UK Addendum which:

(a) Makes reasonable and proportionate changes to the UK Addendum, including correcting errors in the UK Addendum; and/or

(b) reflects changes to UK Data Protection Laws;

(4) The revised UK Addendum will specify the start date from which the changes to the UK Addendum are effective and whether the Parties need to review this Part 3 including the Appendix Information. This Part 3 is automatically amended as set out in the revised UK Addendum from the start date specified.

(5) If the ICO issues a revised UK Addendum under Section 18, if any Party, will as a direct result of the changes in the UK Addendum have a substantial, disproportionate and demonstrable increase in:

(a) its direct costs of performing its obligations under this Part 3; and/or

(b) its risk under this Part 3,

and in either case it has first taken reasonable steps to reduce those costs or risks so that it is not substantial and disproportionate, then that Party may end this Part 2 at the end of a reasonable notice period, by providing written notice for that period to the other Party before the start date of the revised UK Addendum.

(6) The Parties do not need the consent of any third party to make changes to this Part 3, but any changes must be made in accordance with its terms

---

PART 4 – Turkey Cross- Border Transfers

This PART 4 applies where personal data is transferred in accordance with the "KVKK"

In accordance with the requirements of the Turkish law on the Protection of Personal Data No.6698 ("KVKK"), a Turkish translation of this Agreement is provided in Appendix (I).In cases of Turkey Cross-Border Transfers, the data controller shall be responsible for ensuring compliance with KVKK, specifically Article 9, including the submission of the Turkish version of this DPA or any related undertaking to the Turkish Data Protection Authority, where applicable. The Data Processor shall provide reasonable assistance upon the Data Controller's written request but shall have no obligation to submit any documentation to the Authority.

STANDARD CONTRACT TO BE USED FOR THE CROSS-BORDER PERSONAL DATA TRANSFER-2 (DATA CONTROLLER TO DATA PROCESSOR)

SECTION 1-General Provisions

Clause 1-Purpose and Scope

(a) The purpose of this standard contract is to ensure the compliance with provisions of the Law on Personal Data Protection numbered 6698 and dated 24/3/2016 (hereinafter referred to as the "Law") and the Regulation on Procedures and Principles Regarding Cross-Border Personal Data Transfer published in the Official Gazette dated 10/6/2024 and numbered 32598 (hereinafter referred to as the "Regulation")

(b) Data controller transferring the personal data abroad (hereinafter referred to as the"data exporter") and data processor in a third country receiving the personal data from the data exporter (hereinafter referred to as the "data importer") have agreed to this standard contract (hereinafter referred to as the "Contract".

(c) This Contract apply with respect to the transfer of personal data abroad as specified in Annex I.

(d) The Annexes to this Contract (hereinafter referred to as the "Annexes") form an integral part of this Contract.

Clause 2- Effect and Invariability of the Contract

(a) This Contract sets out appropriate safeguards, including enforceable data subject rights and effective legal remedies in the country to which personal data is transferred, to be provided in the cross-border personal data transfer pursuant to the fourth paragraph of Article 9 of the Law and the Regulation, provided that there are no additions, deletions, or modifications.

(b) This Contract is without prejudice to obligations to which the data exporter is subject by virtue of the Law, the Regulation and other relevant legislation.

Clause 3-Rights of Third-Party Beneficiaries

(a) Data subjects may invoke and enforce this Contract, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

i) Clause 1, Clause 2, Clause 3, and Clause 6;

ii) Clause 7.1(b) and Clause 7.9(a), (c), (d) and (e);

iii) Clause 8(a), (c), (d) and (e);

iv) Clause 11(a), (d) and (f);

v) Clause 12.(b) Paragraph (a) is without prejudice to rights of data subjects under the Law.

Clause 4-Interpretation

(a) Where this Contract uses terms that are defined in the Law, the Regulation, and other relevant legislation, those terms shall have the same meaning as in that legislation.

(b) This Contract shall be interpreted in the light of the Law, the Regulation, and other relevant legislation

(c) This Contract shall not be interpreted in a way that conflicts with rights and obligations provided for in the Law, the Regulation, and other relevant legislation.

Clause 5- Hierarchy

In the event of a contradiction between the provisions of this Contract and the provisions of related agreements between the Parties, existing at the time this Contract is agreed or entered into thereafter, the provisions of this Contract shall prevail.

Clause 6- Description of the Transfer

The details of the transfer, including, in particular, the categories of personal data that are transferred, the legal basis of the transfer, and the purpose(s) for which they are transferred, are specified in Annex I.

SECTION II - Obligations of the Parties

Clause 7- Data Protection Safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under this Contract.

Clause 7.1- Instructions

(a) The data importer shall process the personal data only on instructions from the data exporter. The data exporter may give such instructions throughout the duration of the data importer's data processing activities on behalf of the data exporter.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions

Clause 7.2- Being Relevant, Limited, and Proportionate to the Purpose

The data importer shall process the personal data only for the purpose(s) as set out in Annex I in a manner that is relevant, limited, and proportionate.

Clause 7.3- Being Accurate and Kept Up to Date Where Necessary

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to destruct or rectify the data.

Clause 7.4- Duration of Processing and Complete Destruction or Return of Personal Data

Processing by the data importer shall only take place for the duration specified in Annex I. In the event that the data importer's processing of personal data on behalf of the data exporter ceases, the data importer shall, at the choice of the data exporter, return all personal data processed on behalf of the data exporter, along with its copies, to the data exporter, or completely destruct the personal data. The data importer undertakes to ensure compliance with this Contract, even if there are provisions in the legislation that prevent it from fulfilling this obligation, to take necessary technical and administrative measures to ensure the confidentiality of the transferred personal data, and to continue processing activities only to the extent and for as long as required under the legislation. This is without prejudice to Clause 13. The data importer shall document the destruction of the data for the data exporter. Until the data is returned or completely destructed, the data importer shall continue to comply with this Contract.

Clause 7.5- Obligation to Inform

On request, the data exporter shall make a copy of this Contract, including the Annexes as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text by making changes to the Annexes included in the copy to be shared with the data subject. However, the data exporter shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the

Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Article 10 of the Law and the Communique on Procedures and Principles Regarding Compliance with the Obligation to Inform, published in the Official Gazette dated 10/3/2018 and numbered 30356.

Clause 7.6- Security of Data

(a) The data importer and, during transmission, also the data exporter shall implement all necessary technical and organisational measures to ensure the appropriate level of security, depending on the nature of the personal data, in order to prevent unlawful processing, unauthorized access to personal data, safeguard the retention of personal data, and prevent accidental loss, destruction, or damage to personal data. In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purposes of processing and the risks involved in the processing for the data subjects. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the personal data processing that it carries out on behalf of the data exporter, ensuring that only relevant personnel have access to such personal data. The data importer shall ensure that persons authorised to access the personal data do not disclose the obtained data to third parties contrary to this Contract and do not process it for other purposes.

(c) In the event of unauthorized access to personal data processed by the data importer under this Contract, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay. Such notification shall be made using the "Data Breach Notification Form" determined by the Personal Data Protection Board (hereinafter referred to as the "Board") and announced on the official website of the Personal Data Protection Authority (hereinafter referred to as the "Authority"). Where, and in so far as, it is not possible to simultaneously provide all information as stated in the form, this information shall subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under the Law, in particular to notify the Board and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

Clause 7.7- Sensitive Data

(a) The data importer shall apply additional safeguards described in Annex II in line with the sensitive nature of sensitive data.

(b) In the processing of sensitive data, taking adequate measures determined by the Board is also a requirement.

Clause 7.8- Onward Transfers

(a) The personal data transferred to the data importer may only be disclosed by the data importer to a third party located abroad (in the same country as the data importer or in another third country) upon the instruction of the data exporter and in the following cases:

i) the onward transfer is to a country benefitting from an adequacy decision pursuant to first paragraph of Article 9 of the Law;

ii) the third party to whom the onward transfer shall be made ensures appropriate safeguards set out in fourth paragraph of Article 9 of the Law;

iii) the onward transfer is necessary for the establishment, exercise, or defence of legal claims in the context of specific administrative or judicial proceedings;

iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person who is unable to explain his/her consent due to the physical disability or whose consent is deemed legally invalid.

(b) Any onward transfer is subject to compliance by the data importer with all the other safeguards under this Contract, in particular principle to be relevant, limited, and proportionate to the purpose.

(c) If the recipients to the onward transfer are identified prior to notifying the Authority concerning this Contract, these recipients or recipient groups shall be specified in Annex I. Following the notification to the Authority of this Contract, if there are any changes in the recipients or recipient groups to the onward transfer, Annex I shall be updated accordingly, and this situation shall be notified to the Authority.

Clause 7.9-Documentation and Compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under this Contract.

(b) The Parties shall be able to demonstrate compliance with this Contract. The data importer shall keep appropriate information, documentation, and records on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information and documents necessary to demonstrate compliance with the obligations set out in this Contract and at the data exporter's request, allow for and contribute to audits of the processing activities covered by this Contract, at reasonable intervals or if there are indications of noncompliance.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the Board on request.

Clause 8- Sub-Processor

GENERAL WRITTEN AUTHORISATION: (a) The data importer may sub-contract any of its processing activities performed on behalf of the data exporter under this Contract to sub-processor(s) specified in a previously agreed list by the data exporter. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least 15 (fifteen) days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object. The list of sub-processors already authorised by the data exporter can be found in Annex III. Following the notification to the Authority of this Contract, if there are any changes in the sub-processors, Annex III shall be updated accordingly, and this situation shall be notified to the Authority.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations under this Contract, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 7.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to this Contract.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, **including** personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to completely destruct all personal data subject to the transfer or return it alongside its copies.

Clause 9- Data Subject Rights

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under the Law. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 10-Redress

(a) In case of a dispute between a data subject and the data importer as regards the third-party beneficiary rights under this Contract, the data subject may convey their requests to the data importer. The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. The data importer shall deal promptly with any complaints it receives.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with this Contract, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the data subject's rights to lodge a complaint with the Board and to refer the dispute to the competent and authorized courts within the meaning of Clause 18.

(d) The data importer shall undertake to abide by a decision that is binding under the Turkish law.

(e) The data importer agrees that the choice of one of the aforementioned remedies made by the data subject will not prejudice any other rights the data subject may assert under the legislation in force.

Clause 11-Liability

(a) Each Party shall be liable to the other Party for any damages it causes the other Party by any breach of this Contract.

(b) The data importer shall be liable to the data subject. The data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under this Contract.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under this Contract. This is without prejudice to the liability of the data exporter under the Law.

(d) In the event that the data exporter fully compensates the data subject's damages caused by the data importer (or its sub-processor) under paragraph (c), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of this Contract, all responsible Parties shall be severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) If one Party fully compensates the data subject's damages under paragraph (e), it shall be entitled to claim back from the other Party that part of the compensation corresponding to its responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 12-Supervision

The data importer agrees to cooperate with the Authority in any actions and transactions, submit itself to the jurisdiction of the Board, and adhere to the decisions adopted by the Board aimed at ensuring compliance with this Contract. In particular, the data importer agrees to provide the information and documents requested by the Board regarding the subject of the investigation, facilitate on-site inspections when necessary, and comply with the instructions adopted by the Board to rectify any identified legal violations. It shall provide the Board with the information and documents demonstrating that the necessary actions in response to the underlying instructions have been taken.

SECTION III- Local Laws and Obligations in Case of Access by Public Authorities

Clause 13- Local Laws and Practices Affecting Compliance with the Clauses

The data importer agrees, declares, and undertakes that, with respect to the personal data to be transferred under this Contract, there are no national regulations or practices contrary to this Contract. The data importer shall promptly notify the data exporter if, during the duration of this Contract, there is a change in the laws or practices of the third country that is likely to prevent the data importer from fulfilling its undertakings under this Contract and the data importer agrees that the data exporter is entitled to suspend the transfer or terminate this Contract in such a scenario.

Clause 14- Obligations of the Data Importer in case of Access by Public Authorities

The data importer shall promptly notify the data exporter of any requests it receives from a public or judicial authority or it becomes aware of any direct access by public or judicial authorities with respect to transferred personal data pursuant to this Contract. It agrees that the data exporter is entitled, based on the nature of the request or the access, to suspend the transfer or terminate this Contract in such a scenario.

SECTION IV- Final Provisions

Clause 15- Non-Compliance with the Contract and Termination

a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

b) In the event that the data importer is in breach of this Contract or unable to comply with this Contract, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the Contract is terminated. This is without prejudice to Clauses 13 and 14.

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under this Contract, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with this Contract is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of this Contract;

(iii) the data importer fails to comply with a decision of a competent court or the Board regarding its obligations under this Contract. In these cases, the data exporter shall inform the Board.

(d) If the contract is terminated pursuant to paragraph (c), the importer shall at the choice of the data exporter return or destruct the personal data subject to the transfer, along with its copies.The data importer shall continue to ensure compliance with this Contract. The data importer undertakes to continue to ensure compliance with this Contract even if there are provisions in the legislation that prevent it from fulfilling this obligation, to take the necessary technical and administrative measures to ensure the confidentiality of the personal data subject to the transfer, and to continue processing activities only to the extent and for as long as required under that legislation. The data importer shall certify the destruction of the data to the data exporter. Until the data is destructed or returned, the data importer shall continue to ensure compliance with this Contract.

Clause 16- Notification of the Contract to the Authority

Data exporter shall notify the Authority of this Contract within five business days from the completion of signatures.

Clause 17- Governing Law

This Contract shall be governed by Turkish Law.

Cause 18- Forum and Jurisdiction

(a) Any dispute arising from this Contract shall be resolved by the courts of Turkey.

(b) The general provisions shall apply in terms of the forum and the jurisdiction.

(c) The parties agree to the jurisdiction of Turkish courts.

Data Exporter: as stated in the Subscription Agreement

Address: as stated in the Subscription Agreement.

Contact Person's name, title and contact information: as stated in the Subscription Agreement.

Data Importer: Qualifyze GmbH

Address: Bockenheimer Anlage 46, 60322 Frankfurt am Main, Germany

Contact Person's name, title and contact information: as stated above.

ANNEXES

ANNEX I DETAILS OF TRANSFER

Data Exporter's Activities as to Personal Data Transferred Under This Contract

As stated in the DPA.

Data Importer's Activities as to Personal Data Transferred Under This Contract

As stated in the DPA.

Category or Categories of Data Subjects

As stated in the DPA.

Categories of Personal Data Transferred

As stated in the DPA.

Sensitive Data Transferred (If Applicable)

As stated in the DPA.

Legal Basis of Transfer

As stated in the DPA.

The Frequency of the Transfer (e.g. whether the data is transferred on a one-off or continuous basis)

As stated in the DPA.

Nature of the processing

As stated in the DPA.

Purpose(s) of the Data Transfer and Further Processing

As stated in the DPA.

The Period for Which the Personal Data Will Be Retained

As stated in the DPA.

Recipients or Recipient Groups

As stated in the DPA.

Data Exporter's Data Controllers' Registry Information System (VERBIS) Information (If there is an obligation to register)

As stated in the Subscription Agreement and the DPA above.

ANNEX II- TECHNICAL AND ORGANIZATIONAL MEASURES

(In cases of transferring sensitive data, the technical and administrative measures taken regarding such data shall be specified separately)

As stated in Appendix II.

ANNEX III- LIST OF SUB-PROCESSORS

The controller has authorised the use of the sub-processors included in Appendix III